

Social Media and Identity Theft Implications on Nigerian Victims and International Economy

Tolulope Kayode-Adedeji

Covenant University, Nigeria

Obianuju Victoria Okeke

Covenant University, Nigeria

Lanre Amodu

Covenant University, Nigeria

Opeyemi Fasanya

Covenant University, Nigeria

Nelson Okorie

Covenant University, Nigeria

INTRODUCTION

In this 21st century and beyond, many can attest to the role of ICT in the development of communication in the world. According to Adaja and Ayodele (2013 p. 65), ‘one of the developments in Information and Communication Technology in the 21st century was the finding and advent of the new media which have enabled the formation of several channels of social communication.’

As a result of the fast-growing technology, in social communication, there has been dependence on the internet by a large percentage of individuals around the world.

Consequently, personal information is shared when creating profiles on social media platforms thereby making it easy for online crimes to take place. Security attacks such as hacking, identity theft, phishing scams, viruses are now common online as users share their names, date of birth, the name of schools, family information, and others on social media sites.

While activities online increase, there are concerns about the ways personal information shared by social media users may be collected and analysed (Hinduja and Patchin, 2009). According to Walker (2016) the state of the net poses, that more than half of the people using social media applications share private information about themselves online, exposing themselves to online dangers. The findings reveal that: 25% of persons with a *Facebook* account do not use the site’s privacy control or are not aware of them, 40% of social media users post their personal identity information online, exposing them to identity theft and 9% of social media users dealt with a form of abuse within the past year (e.g., malware, online scams, identity theft or harassment) (Finch, 2003).

Due to this increase, there seems to be a connection between the usages of such media with identity theft, cyberbullying, online sexual predators mainly affected youths because of lack of security consciousness and privacy about personal information (Jegede, et, al; (2016) McGillivray, 2015). Also,

DOI: 10.4018/978-1-5225-9715-5.ch055

committing identity fraud with the help of the Internet may be more accessible and more efficient for criminals than ever before (Milne et al, 2004).

Emily Finch, the author of “What a Tangled Web We Weave: Identity Theft and the Internet,” believes that social media users are “less security-minded about their personal information when they are online than they are in ‘real life’ situations.” This is true because when people are on social media sites, they reveal information online that they would not show to someone in real life situation. It is therefore easy to understand how this information is wrongly used and leads to identity theft (Finch, 2003).

Identity theft did not begin over the Internet. Before the use of internet became popular, fraudsters stole people’s identities by going through their documents. They also used their mobile devices to commit such fraud. In Nigeria, before the prominence of the internet, there were fraudsters commonly called 419’ers, and these fraudsters duped mostly big men and women who lived in Lagos (Ezea, 2017).

With the acceptance of internet, identity theft is becoming more popular around the world. According to Federal Trade Commission, identity theft was the number one fraud in 2008. Now with its popularity, different online fraudulent activities have become the norm over the years.

However, Nigeria social media users continue to fall, a victim of this fraudulent activities, as they continue to imbibe the culture of registration and to use newly established social media network with more existing features (Omodunbi et al., 2016)

Therefore, diverse investigation abounds on the issue of social media identity theft. Selwyn (2004) examined how older adult employed the uses of social media to lower perceived life stress thereby making them victims of social media identity theft. On the other hand, Rezmik (2013) investigates the dominant methods used in carrying out social media identity theft on social media networking site. They further stress the need for the Federal Governments to be solely responsible for the protection of social media users by ensuring the perpetrators are punished (Al-Daraish et al., 2014). Most importantly, Milne et al., (2004) discussed online behaviours that lead to identity theft to create awareness for online security for social media users.

To this end, Kayode-Adedeji et al., (2017) emphasized the need for regulating the social media, while Adu et al., (2014) further reviewed the different security and privacy risk threatening online social network users and proposed several systems that enable internet users’ activities to be monitored. Little research, however, has been done on the implication and users’ awareness of the necessary security measures social media users can put in place to avoid being a victim of social media identity theft.

Considering the differences that exist in countries, regarding the culture of communication on social media, the results emanating from this investigation gives a future opportunity for a comparative study serving as a guideline or map in the development of policies for future cybersecurity as emphasised by Peters (2017).

So, this research attempts to find out the implications of this crime on the victims, to ascertain if people are aware of this crime, to educate people on avoiding social media identity theft and also the reasons for such fraud.

ICT IN THE PRESENT AGE

Information and Communication Technology (ICT) inventions on the cyberspace remains over-whelming as more platforms are created to allow for diverse activities. There has also been applications (Apps), and websites, enhanced by new features on already existing internet environment. Communication technology has allowed the use of social media platforms, new features on gadgets, solar-powered drones,

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/social-media-and-identity-theft-implications-on-nigerian-victims-and-international-economy/248086

Related Content

Interpreting for Victims of Violence: Its Impact on Victims and Interpreters

Lois M. Feuerle (2022). *Research Anthology on Child and Domestic Abuse and Its Prevention* (pp. 779-811).

www.irma-international.org/chapter/interpreting-for-victims-of-violence/301184

Regulating the Internet

David T. A. Wesley (2020). *Encyclopedia of Criminal Activities and the Deep Web* (pp. 392-401).

www.irma-international.org/chapter/regulating-the-internet/248055

The Role of the Pediatric Healthcare System in Preventing, Identifying, and Responding to Child Trafficking

Carmelle Wallace, Kara Huls, Charli Cohen and Kathleen Vincent (2022). *Paths to the Prevention and Detection of Human Trafficking* (pp. 170-202).

www.irma-international.org/chapter/the-role-of-the-pediatric-healthcare-system-in-preventing-identifying-and-responding-to-child-trafficking/304617

Web-Based Child Sexual Exploitation

Lacey Nicole Wallace (2020). *Encyclopedia of Criminal Activities and the Deep Web* (pp. 533-546).

www.irma-international.org/chapter/web-based-child-sexual-exploitation/248066

Underground Cyber Economy and the Implication for Africa's Development: A Theoretical Overview

Okhuevbie James Olu (2020). *Global Perspectives on Victimization Analysis and Prevention* (pp. 175-189).

www.irma-international.org/chapter/underground-cyber-economy-and-the-implication-for-africas-development/245035